#2/3-6-02

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION of
Inventor(s): RELANDER et al.

Appln. No.: 09 | ↑ Serial No.
Series Code ↑

Group Art Unit: Not Yet Assigned

Filed: November 19, 2001

Examiner: Not Yet Assigned

Title: MAINTAINING END-TO-END SYNCHRONIZATION ON TELECOMMUNICATIONS CONNECTION

Atty. Dkt. P 284077 | 2000934US/Lt/kp
M# Client Ref

Date: November 19, 2001

SUBMISSION OF PRIORITY DOCUMENT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 55

Hon. Asst Commissioner of Patents
Washington, D.C. 20231

Sir:

Please accept the enclosed certified copy(ies) of the respective foreign application(s) listed below for which benefit under 35 U.S.C. 119/365 has been previously claimed in the subject application and if not is hereby claimed.

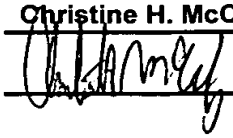
Application No.	Country of Origin	Filed
20002607	FINLAND	November 28, 2000

Respectfully submitted,

Pillsbury Winthrop LLP
Intellectual Property Group

1600 Tysons Boulevard
McLean, VA 22102
Tel: (703) 905-2000

By Atty: Christine H. McCarthy **Reg. No.** 41844

Sig: 

Fax: (703) 905-2500
Tel: (703) 905-2143

Atty/Sec: CHM/JRH

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 2.11.2001

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija Applicant	**Nokia Networks Oy** **Helsinki**
Patenttihakemus nro Patent application no	**20002607**
Tekemispäivä Filing date	**28.11.2000**
Kansainvälinen luokka International class	**H04L**

Keksinnön nimitys
Title of invention

"Päästä-päähän -tahdistuksen ylläpitäminen tietoliikenneyhteydellä"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

Maksu 300,- mk
Fee 300,- FIM

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1782/1995 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1782/1995 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A, P.O.Box 1160, FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

Päästä-päähän -tahdistuksen ylläpitäminen tietoliikenneyhteydellä

Keksinnön tausta

Keksintö liittyy menetelmään ja laitteeseen päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä.

Tietoliikennejärjestelmissä kuten viranomaisverkossa on erittäin tärkeää, ettei liikenteen salakuuntelu ole mahdollista. Ilmatierajapinta on tyypillisesti salattu, joten vaikka radioliikennettä valvotaan, ulkopuolinen ei pysty purkamaan sitä. Infrastruktuurissa liikennettä ei kuitenkaan välttämättä salata, joten liikenne kuten puhe voidaan purkaa käyttäen kyseisen järjestelmän koodekkia. Vaikka ulkopuolinen ei periaatteessa pysty kuuntelemaan puhevuota infrastruktuurin sisältä, tämä on kuitenkin vaativimmille käyttäjille mahdollinen turvallisuusriski. Siksi on kehitetty ratkaisu, jossa puhe voidaan salata päästä-päähän -salauksella. Esimerkkinä päästä-päähän -salauksen mahdollistavasta järjestelmästä on TETRA-järjestelmä (TErrestrial Trunked RAdio).

Päästä-päähän -salauksen perusajatuksena on se, että verkon käyttäjä kuten viranomaisorganisaatio suorittaa liikenteen salauksen ja salauksen purun itsenäisesti ja käytettävästä siirtoverkosta riippumattomasti esimerkiksi päätelaitteiden yhteydessä.

Esimerkiksi TETRA-järjestelmässä päästä-päähän -salausta käytettäessä lähettäjä koodaa ensin 60 ms:n ääninäytteen TETRA-koodekkia käyttäen, josta syntyy selväkielinen näyte. Lähettävä päätelaite luo tiettyä avainsarjaa käyttäen salatun näytteen. Salattu näyte lähetetään sitten verkolle. Vastaanottaja purkaa salatun näytteen käyttämällä samaa avainsarjaa, jolloin saadaan taas selväkielinen näyte.

Salauksen murtamisen ehkäisemiseksi avainsarjaa muutetaan jatkuvasti, joten jokainen 60 ms:n ääninäytteen käsittävä kehys on salattu omalla avainsarjallaan. Molempien avainsarjakehittimien on siis sovittava siitä, mitä avainsarjaa on käytettävä jokaiselle kehykselle. Tämä tehtävä kuuluu tahdistuksen ohjaukselle. Tehtävää varten käytetään tahdistusvektoreja, joita lähetetään päätelaitteiden välillä puhekaistalla olevan signaalin avulla.

Avainsarjakehitin luo avainsarjan tietyn avaimen ja alustusvektorin perusteella. Avaimet jaetaan jokaiselle päätelaitteelle, joka osallistuu salattuun puheluun. Tämä on osa päätelaitteen asetuksia. Uusi avainsarja luodaan siis kerran 60 millisekuntia kohti. Jokaisen kehyksen jälkeen alustusvektoria muutetaan. Yksinkertaisin vaihtoehto on inkrementoida sitä yhdellä, mutta jokainen

salausalgoritmi päättää itse inkrementointitavastaan, joka voi olla monimutkaisempikin salausten murtamisen ehkäisemiseksi.

Tahdistusohjauksen tehtävä on varmistaa, että molemmat päät tietävät, millä alustusvektorilla kukin kehys on salattu. Jotta salaaja ja avaaja pääsisivät yhteisymmärrykseen alustusvektorin arvosta, puheenvuoron alussa lähetetään tahdistusvektori. Joskus kyseessä saattaa olla myös ryhmäpuhelu, johon on voitava liittyä puheenvuoron aikanakin. Tämän vuoksi tahdistusvektoria lähetetään jatkuvasti esimerkiksi 1-4 kertaa sekunnissa. Tahdistusvektori sisältää alustusvektorin lisäksi mm. avaimen tunnuksen ja CRC-virheentarkastuksen, joten päätelaite voi varmistaa tahdistusvektorin eheyden. Vastaanottaja laskee siis kuinka monta kehystä on lähetetty tahdistusvektorin jälkeen ja avainsarjakehitin luo uuden alustusvektorin viimeksi vastaanotetun alustusvektorin ja kehysten lukumäärän perustella.

Tiedonsiirtoverkko saattaa käsittää yhden tai useampia pakettikytkettyjä yhteyksiä, esimerkiksi IP (Internet Protocol) -yhteyksiä, joissa tieto siirretään esimerkiksi IP-puhetekniikalla (voice over IP, VoIP). Eräs standardiprotokolla tosiaikaisen tiedon kuten äänen ja videokuvan siirtämiseen esimerkiksi IP-verkossa on RTP (Real Time Protocol). IP-verkko aiheuttaa tyypillisesti vaihtelevan viiveen pakettien siirrossa. Esimerkiksi puheen ymmärrettävyyden kannalta viiveen vaihtelu on hyvin haitallista. Tämän korvaamiseksi RTP siirron vastaanottopää puskuroi tulevat paketit jitterpuskuriin ja toistaa ne tiettyyn toistoaikaan. Ennen toistohetkeä tullut paketti osallistuu alkuperäisen signaalin uudelleen rakentamiseen. Toistohetken jälkeen tullut paketti on käyttämätön ja hylätty.

Tosiaikainen sovellus vaatii toisaalta mahdollisimman pienen päästä-päähän -viiveen, ja näin halutaan pienentää toistoviivettä. Toisaalta pitkä toistoviive sallii pitkän ajan pakettien saapumiselle, ja näin voidaan hyväksyä enemmän paketteja. Toistoviiveen arvoa on näin säädettävä jatkuvasti verkon olosuhteiden mukaan. Useimmilla RTP-algoritmeilla on toiminne, joka säätää toistoviiveen automaattisesti verkko-olosuhteiden mukaan äänen laadun parantamiseksi. Toistoviiveen siirtäminen esimerkiksi 60 ms eteenpäin tapahtuu siten, että IP-yhdyskäytävä luo 60 ms:n korvaavan paketin. Toisin sanoen lisätään siirrettävän kehysvuon sisälle ylimääräinen kehys. Toistoviiveen siirtäminen taaksepäin tapahtuu siten, että ainakin yksi kehys hävitetään.

Ongelmana yllä kuvatussa järjestelyssä on se, että jos käytetään tahdistettua päästä-päähän -salauskoodausta ja kehysvuohon lisätään ylimää-

räinen kehys, on tämän seurauksena vastaanottopään kehyslaskuri yhden kehyksen etuajassa verrattuna tuleviin kehyksiin eikä vastaanottopään avainsarja enää vastaa lähetyspään avainsarjaa. Vastaavasti, jos kehysvuosta poistetaan kehys on vastaanottopään kehyslaskuri yhden kehyksen myöhässä verrattuna tuleviin kehyksiin ja avainsarja ei enää vastaa lähetyspään avainsarjaa.

Toistoviiveen siirtämisellä esimerkiksi puheenvuoron keskellä on siis se seuraus, että päästä-päähän -tahdistus menetetään, eikä salattu puhe ole enää dekoodattavissa. Tämä jatkuu kunnes lähetyspää lähettää uuden tahdistusvektorin, joka tahdistaa vastanottopään. Tämä ilmiö voidaan välttää siten, että esimerkiksi semidupleksipuheluissa toistoviivettä vaihdetaan vain puheenvuorojen jälkeen. Jos puheenvuorot ovat pitkiä, voidaan toistoviivettä tällöin muuttaa epäedullisen harvoin: puheenlaatu saattaa olla huono koko puheenvuoron loppuun asti, koska toistoviivettä ei voida vaihtaa aiemmin. Edelleen esimerkiksi dupleksipuheluissa, joissa ei ole puheenvuoroja ja joissa päätelaite lähettää jatkuvasti, toistoviivettä ei voida vaihtaa ollenkaan koko puhelun aikana, jos halutaan välttää tahdistuksen menetys.

Keksinnön lyhyt selostus

Keksinnön tavoitteena on siten kehittää menetelmä ja menetelmän toteuttava laitteisto siten, että yllä mainitut ongelmat saadaan ratkaistua. Keksinnön tavoite saavutetaan menetelmällä ja järjestelmällä, joille on tunnusomaista se, mitä sanotaan itsenäisissä patenttivaatimuksissa 1, 7 ja 13. Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksintö perustuu siihen, että jos toistoviivettä muutetaan tiedon lähetyksen kuten puheenvuoron tai puhelun aikana, valitaan muutosajankohta siten, että muutoksen jälkeen seuraavaksi siirtyvä kehys käsittää tahdistusvektorin, jolloin vastaanottopää tahdistuu välittömästi muutoksen jälkeen ja tiedon salauksen purkuun ja siten dekoodaukseen ei tule aukkoja.

Keksinnön mukaisen menetelmän ja järjestelmän etuna on se, että ne mahdollistavat toistoviiveen muuttamisen myös tiedon lähetyksen aikana ilman, että tämän seurauksena salatun tiedon dekoodaus häiriintyisi.

Kuvioiden lyhyt selostus

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joista:

Kuvio 1 esittää lohkokaavion TETRA-järjestelmän rakenteesta;

Kuvio 2 esittää lohkokaavion päästä-päähän -salauksen toiminnasta;

Kuvio 3 esittää vastaanottajan suorittamaa alustusvektorin laskemista;

Kuvio 4 esittää kaavion RTP-paketin rakenteesta;

Kuvio 5 esittää RTP-algoritmin toimintaa;

Kuvio 6 esittää kaavion RTP-pakettien tulotodennäköisyydestä siirtoajan funktiona;

Kuvio 7A esittää kaavion toistoviiveen lyhentämisestä ja

Kuvio 7B esittää kaavion toistoviiveen kasvattamisesta.

Keksinnön yksityiskohtainen selostus

Keksintöä on seuraavassa kuvattu esimerkinomaisesti TETRA-järjestelmän yhteydessä. Keksintöä ei kuitenkaan ole tarkoitus rajoittaa mihinkään tiettyyn tietoliikennejärjestelmään tai tiedonsiirtoprotokollaan. Keksinnön sovellukset myös muihin järjestelmiin ovat alan ammattimiehelle ilmeisiä.

Kuviossa 1 on esitetty esimerkki TETRA-järjestelmän rakenteesta. Vaikka kuviossa ja seuraavassa selityksessä on viitattu TETRA-järjestelmän mukaisiin verkkoelementteihin, ei tämä mitenkään rajoita keksinnön soveltamista myös muihin tietoliikennejärjestelmiin. On huomattava, että kuviossa on esitetty vain keksinnön ymmärtämisen kannalta olennaisia elementtejä ja järjestelmän rakenne saattaa poiketa esitetystä ilman, että sillä on merkitystä keksinnön perusajatuksen kannalta. On myös huomattava, että todellisessa matkaviestinjärjestelmässä voi kutakin elementtiä olla mielivaltainen määrä. Päätelaitteet MS (Mobile Station) ovat yhteydessä tukiasemiin TBS (TETRA Base Station) radioteitse. Päätelaitteet MS voivat myös ns. suorakanavamoodissa viestiä suoraan keskenään käyttämättä tukiasemia TBS. Jokainen tukiasema TBS on kytketty yhteysjohdolla johonkin kiinteän siirtoverkon TETRA-keskuksista DXT (Digital Exchange for TETRA). TETRA-keskukset DXT on kytketty kiinteällä yhteydellä toisiin keskuksiin ja TETRA-solmukeskukseen DXTc (Digital Central Exchange for TETRA, ei esitetty), joka on keskus, johon on kytketty muita keskuksia DXT ja/tai muita solmukeskuksia DXTc vaihtoehtoisten liikennereittien aikaansaamiseksi. Mahdolliset ulkoiset liitäntärajapinnat esimerkiksi yleiseen puhelinverkkoon PSTN (Public Switched Telephone Network), digitaaliseen monipalveluverkkoon ISDN (Integrated Services Digital Network), yritysvaihteeseen PABX (Private Automatic Branch Exchange) ja

pakettivälitteiseen dataverkkoon PDN (Packet Data Network) voivat sijaita yhdessä tai useammassa keskuksessa DXT. Edellä mainituista liitäntärajapinnoista on kuviossa esitetty liitäntä pakettivälitteiseen dataverkkoon PDN yhdyskäytävän GW avulla. Yhdyskäytävän GW tehtävä on muuttaa keskukselta DXT tuleva piirikytketty data pakettiverkkoon PDN meneväksi pakettikytketyksi dataksi ja päinvastoin. Pakettivälitteiseen dataverkkoon PDN kytketty päätelaite TE voi näin olla yhteydessä TETRA-verkkoon. Yhdyskäytävä GW voi olla erillinen verkkoelementti tai esimerkiksi keskuksen DXT osa. Lisäksi kuviossa on esitetty keskukseen DXT kytketty käyttöpaikkajärjestelmä DS (Dispatcher System), joka muodostuu käyttöpaikan ohjaimesta DSC (Dispatcher Station Controller) ja siihen liitetystä työasemasta DWS (Dispatcher Workstation). Käyttöpaikanhoitaja ohjaa päätelaitteiden MS puheluita ja muita toimintoja työaseman DWS välityksellä.

Kuviossa 2 on havainnollistettu päästä-päähän -salauksen toimintaa. Päästä-päähän -salausta käytettäessä lähettäjä 20 koodaa ensin 60 ms:n ääninäytteen TETRA-koodekkia käyttäen, josta syntyy selväkielinen näyte (P). Päätelaite luo P:n pituista avainsarjaa (KSS, Key Stream Segment) avainsarjakehittimessä 21. Salattu näyte (C) saadaan suorittamalla binäärinen XOR-operaatio lohkossa 22:

$$C = P \text{ xor } KSS$$

Salattu näyte lähetetään sitten siirtoverkolle 29. Vastaanottaja 30 suorittaa saman XOR-operaation lohkossa 28 käyttämällä samaa avainsarjaa, josta syntyy taas selväkielinen näyte P.

$$P = C \text{ xor } KSS$$

Salauksen murtamisen ehkäisemiseksi avainsarjaa KSS muutetaan jatkuvasti, joten jokainen kehys on salattu omalla avainsarjallaan. Molempien avainsarjakehittimien 21 ja 27 on siis sovittava siitä, mitä avainsarjaa on käytettävä kullekin kehykselle. Tämä tehtävä kuuluu tahdistuksen ohjaukselle 23 ja 26. Tehtävää varten käytetään tahdistusvektoreja, joita lähetetään päätelaitteiden välillä puhekaistalla olevan signaalin avulla.

Avainsarjakehitin (EKSG, Encryption Key Stream Generator) 21 ja 27 luo avainsarjan (KSS) salausavaimen (CK, Cipher Key) ja alustusvektorin (IV) perusteella. Uusi avainsarja luodaan siis kerran 60 millisekuntia kohti.

KSS = EKSG (CK, IV)

Jokaisen kehyksen jälkeen alustusvektoria muutetaan. Yksinkertaisin vaihtoehto on inkrementoida sitä yhdellä, mutta jokainen salausalgoritmi päättää itse inkrementointitavastaan, joka voi olla monimutkaisempikin salausten murtamisen ehkäisemiseksi.

Tahdistusohjauksen 23 ja 26 tehtävä on varmistaa, että molemmat päät 20 ja 30 tietävät, millä alustusvektorilla jokainen kehys on salattu. Jotta salaaja 20 ja avaaja 30 pääsisivät yhteisymmärrykseen alustusvektorin arvosta, puheenvuoron alussa lähetetään tahdistusvektori (SV). Joskus kyseessä saattaa olla myös ryhmäpuhelu, johon on voitava liittyä puheenvuoron aikanakin. Tämän vuoksi tahdistusvektoria lähetetään jatkuvasti n. 1-4 kertaa sekunnissa. Tahdistusvektori sisältää alustusvektorin lisäksi mm. avaimen tunnuksen ja CRC-virheentarkastuksen, joten päätelaite voi varmistaa tahdistusvektorin eheyden.

Vastaanottaja 30 laskee siis kuinka monta kehystä (n) on lähetetty tahdistusvektorin jälkeen. Vastaanottajan 30 avainsarjakehitin 27 luo uuden alustusvektorin IV viimeksi vastaanotetun alustusvektorin ja kehysten lukumäärän perustella. Vastaanottajan suorittamaa alustusvektorin IV laskemista on havainnollistettu kuviossa 3, jossa on esitetty siirrettävä kehysjono. Esitetyssä jonossa kehykset 1, 6, 12 ja 13 sisältävät tahdistusvektorin SV, joissa ilmoitetaan alustusvektorin IV numero.

Molempien päiden 20 ja 30 on sovittava siitä, miten puhelu salataan. Tahdistuksen ohjausyksiköt 23 ja 26 molemmissa päissä kommunikoivat keskenään U-varastettujen puhelohkojen avulla. Lähettävä päätelaite käyttää hyväkseen yhtä tai kahta puhelohkoa kehyksen sisältä omaan tarkoitukseensa. Tämä tapahtuu lohkossa 24. Tämä ilmaistaan vastaanottavalle päätelaitteelle asettamalla tarkoituksenmukaisesti 3 ensimmäistä ohjausbittiä kehyksen sisällä. Siten infrastruktuuri 29 ymmärtää, että kyseessä on päätelaitteesta-päätelaitteeseen-tieto, ja se siirtää tietoja sen perusteella läpinäkyvästi muuttamatta niitä. Sen lisäksi vastaanottava päätelaite havaitsee, ettei ko. puhelohkossa ole puhetietoja, eikä välitä niitä koodekille, vaan käsittelee niitä tar-

koituksenmukaisesti, toisin sanoen lohkossa 25 suodatetaan tahdistuksenohjaustieto tahdistuksenohjaukselle 26, ja luo korvaavan äänen varastetun puheen sijaan. Puhelohkon varastaminen hävittää 30 ms pituisen puheen. Tämä aiheuttaisi tauon puheessa, joten sen laatu huononisi ja sitä olisi vaikeampi ymmärtää. Tämän välttämiseksi TETRA-koodekki sisältää korvausmekanismin. Todellisuudessa käyttäjä ei koe puheen puuttumista haitallisena, mikäli puhelohkoja ei varasteta enemmän kun 4 kertaa sekunnissa. Salausavaimet CK jaetaan jokaiselle päätelaitteelle, joka osallistuu salattuun puheluun. Tämä on osa päätelaitteen asetuksia.

Kuviossa 1 esitetty pakettikytkentäinen dataverkko PDN voi olla esimerkiksi Internet, jossa käytetään TCP/IP protokollia. TCP/IP on tiedonsiirtoprotokollaperheen nimi, jota käytetään lähiverkon sisällä tai lähiverkkojen välillä. Protokollat ovat IP (Internet-protokolla), kuljetusprotokolla TCP (Transmission Control Protocol) ja tietosähkeprotokolla UDP (User Datagram Protocol). Perheeseen kuuluu myös muita protokollia tiettyjä palveluja, kuten tiedostosiirtoa, sähköpostia, etäkäyttöä ym., varten.

TCP/IP-protokollat on jaettu kerroksiin: yhteyskerros, verkkokerros, kuljetuskerros ja sovelluskerros. Yhteyskerros vastaa päätelaitteen fyysisestä liittymisestä verkkoon. Se koskee lähinnä verkkokorttia ja ajuria. Verkkokerrosta kutsutaan usein Internet- tai IP-kerrokseksi. Kerros vastaa pakettien siirtämisestä verkon sisällä ja mm. reitityksestä koneesta toiseen IP-osoitteen perusteella. IP tarjoaa TCP/IP-protokollaperheessä verkkokerroksen. Kuljetuskerros tarjoaa datavuopalvelun kahden päätelaitteen välillä sovelluskerrosta varten ja ohjaa vuot päätelaitteessa oikeaan sovellukseen. Internetprotokollassa on kaksi siirtoyhteyskäytäntöä: TCP ja UDP. Siirtokerroksen toinen tehtävä on ohjata paketit oikeaan sovellukseen porttinumeroiden perusteella. TCP tarjoaa luotettavan datavuon päätelaitteesta toiseen. TCP pilkkoo datan sopivankokoisiksi paketeiksi, kuittaa vastaanotetut paketit ja valvoo, että lähetetyt paketit kuitataan vastaanotetuiksi toisessa päässä. TCP vastaa luotettavasta siirrosta päästä-päähän, eli sovelluksen ei tarvitse huolehtia siitä. UDP on toisaalta paljon yksinkertaisempi protokolla. UDP ei vastaa tietojen perilletulosta, vaan tätä vaadittaessa sovelluskerroksen on huolehdittava siitä. Sovelluskerros vastaa kunkin sovelluksen omasta tiedonkäsittelystä.

RTP on Internetin standardiprotokolla tosiaikaisen tiedon, kuten äänen ja videokuvan siirtämiseen. Sitä voidaan käyttää mediatilauspalvelua tai vuorovaikutteista palvelua kuten IP-puheluita varten. RTP koostuu media-

osasta ja ohjausosasta. Jälkimmäistä kutsutaan RTCP:ksi (Real Time Control Protocol). RTP:n mediaosasta löytyy tukea tosiaikaisille sovelluksille. Tämä sisältää aikatuen, kadon havaitsemisen, turvallisuustuen ja sisällön tunnistamisen. RTCP mahdollistaa tosiaikaiset konferenssit erikokoisten ryhmien sisällä ja sen lisäksi päästä-päähän -palvelun laadun arvioinnin. Se tukee myös useamman mediavuon tahdistusta. RTP on suunniteltu siirtoverkosta riippumattomaksi, mutta Internet-verkossa RTP käyttää yleensä IP/UDP:tä. RTP-yhteyskäytännöllä on monia piirteitä, jotka mahdollistavat päästä-päähän tosiaikaisen tiedonsiirron. Jokaisessa päässä audiosovellus lähettää säännöllisesti audiotietoja pieninä näytteinä, jotka voivat olla pituudeltaan esimerkiksi 30 ms. Jokaiseen näytteeseen liitetään RTP-otsikko. RTP-otsikko ja tiedot taas pakataan UDP- ja IP-pakettiin.

RTP-otsikossa tunnistetaan paketin sisältö. Tämän kentän arvoa käyttämällä ilmaistaan, mitä koodausmenetelmää käytetään (PCM, ADPCM, LPC jne.) RTP-paketin hyötykuormassa. Internetissä, kuten muissa pakettiverkoissa, paketit voivat saapua mielivaltaisessa järjestyksessä, myöhästyä vaihtelevan ajan tai jopa kadota kokonaan. Tämän estämiseksi jokaiselle paketille tietyssä vuossa annetaan oma järjestysnumero ja aikaleima, jonka perusteella vastaanotettu vuo järjestyy uudelleen alkuperäisen vuon mukaan. Järjestysnumeroa kasvatetaan yhdellä jokaista pakettia kohti. Järjestysnumeroiden avulla vastaanottaja pystyy havaitsemaan puuttuvan paketin ja myös arvioimaan pakettihukan.

Aikaleima on 32 bittinen numero. Sillä ilmaistaan näytteenoton aloitushetki. Sen laskemiseen on käytettävä monotonisesti ja lineaarisesti ajan mukana kasvavaa kelloa. Kellon taajuus on valittava siten, että se on sisällölle sopiva, tarpeeksi nopea värinän laskemiseksi ja tahdistuksen mahdollistamiseksi. Esimerkiksi käytettäessä PCM-A-laki-koodaustapaa kellotajuus on 8000 Hz. Lähetettäessä 240-tavun pituisia RTP-paketteja, joka vastaa 240 PCM-näytettä, aikaleimaa kasvatetaan 240:llä jokaista pakettia kohti. RTP-otsikon pituus on 3 - 18 sanaa (32-bittinen sana). Kuviossa 4 on havainnollistettu RTP-paketin muotoa. Kenttien merkitys on seuraava: V: versio; käytetty RTP:n versio, nykyisin 2. Täyte: paketissa on täytetavuja; viimeinen tavu ilmoittaa, montako. Laajennus: paketin jälkeen tasan yksi otsakelaajennus. PM: palvelulähteiden määrä ilmoittaa, monenko lähteen tuottamaa informaatiota paketissa on. Merkitsintä voidaan käyttää ilmoittamaan merkittävistä tapahtumista esimerkiksi kehysten rajoista. HT: hyötykuorman tyyppi ilmoittaa hyötykuor-

massa olevan median tyypin. Sarjanumeroa kasvatetaan yhdellä jokaista lähetettyä datapakettia kohti. Se auttaa havaitsemaan pakettihukan ja epäjärjestyksen. Alkuarvo on satunnainen. Aikaleima kertoo ensimmäisen tavun näytteistyshetken. Sitä käytetään tahdistukseen ja värinän laskemiseen. Alkuarvo on satunnainen. SSRC: satunnaisesti valittu tahdistuslähteen tunniste. Ilmoittaa lähteiden yhdistyspisteen tai alkuperäisen lähettäjän, jos on vain yksi lähde. CSRC-lista tässä paketissa mukana olevien lähteiden lista.

Internet aiheuttaa vaihtelevan viiveen äänipakettien siirrossa. Puheen ymmärrettävyyden kannalta viiveen vaihtelu on hyvin haitallista. Tämän korvaamiseksi RTP:n vastaanottopää puskuroi tulevat paketit jitterpuskuriin ja toistaa ne tiettyyn toistoaikaan. Ennen toistohetkeä tullut paketti osallistuu alkuperäisen signaalin uudelleen rakentamiseen. Toistohetken jälkeen tullut paketti on käyttämätön ja hylätty.

Kuvio 5 havainnollistaa RTP-algoritmin toimintaa. Kuviossa kirjain t viittaa paketin lähetysajankohtaan, kirjain a vastaanottoajankohtaan ja p toistoajankohtaan. Yläindeksit ilmaisevat paketin numeroa ja alaindeksit puheenvuoron numeroa. K:nnessa puheenvuorossa paketit saapuvat vastaanottopäähän vaihtelevan siirtoajan jälkeen. RTP-algoritmi toistaa ne sitten oikealla hetkellä. (K+1):nnessä puheenvuorossa paketit 1 ja 2 vaihtelevat järjestystä, ja paketti 4 saapuu toistohetkensä jälkeen, joten se hylätään. RTP-algoritmi palauttaa paketit oikeaan järjestykseen, toistaa ne oikealla hetkellä, ja ilmaisee esimerkiksi korjaustoimenpiteitä varten, mitkä paketit puuttuvat tai ovat myöhästyneet. Toistoviive on aika t(toistoviive) = t(toisto) – t(lähetys). RTP-algoritmi huolehtii siitä, että toistoviive jää vakioksi koko puhevuoron aikana.

IP-paketin viive IP-verkon läpi t=t(tulo) – t(lähtö) koostuu kahdesta tekijästä. L on kiinteä viive, joka riippuu siirtoajasta ja keskimääräisestä jonotusajasta. J on taas vaihteleva viive, joka riippuu vaihtelevasta jonotusajasta IP-verkon sisällä, ja joka aiheuttaa jitterin. IP-verkon vastaanottopäässä on jitterpuskuri, joka tallentaa paketit muistiinsa, mikäli siirtoaika t < t(toistoviive). Toistoviiveen määritteleminen on kompromissiratkaisu. Tosiaikainen sovellus vaatii toisaalta mahdollisimman pienen päästä-päähän -viiveen, ja näin halutaan pienentää toistoviivettä. Toisaalta pitkä toistoviive sallii pitkän ajan pakettien saapumiselle, ja näin voidaan hyväksyä enemmän paketteja. Toistoviiveen arvoa on näin säädettävä jatkuvasti verkon olosuhteiden mukaan. Kuvio 6 havainnollistaa tätä. Paketti, jonka siirtoaika t < L+ J voidaan hyväksyä, kun taas paketti, jonka siirtoaika t > L + J on hylättävä. Kasvattamalla J:tä voidaan

näin kasvattaa hyväksyttyjen pakettien määrää. Toistoviivettä voidaan säätää esimerkiksi aloittamalla pienellä arvolla, ja kasvattamalla sitä säännöllisesti, kunnes myöhässä olevien pakettien osa jää tietyn rajan, esimerkiksi 1%, alle.

Useimmilla RTP-algoritmeilla on toiminne, joka säätää toistoviiveen automaattisesti verkko-olosuhteiden mukaan äänen laadun parantamiseksi. Toistoviiveen siirtäminen esimerkiksi 60 ms eteenpäin tapahtuu siten, että RTP-vastaanotossa luodaan 60 ms:n korvaava puhepaketti ennen kun puhevuo jatkuu. Toisin sanoen lisätään puhevuon sisälle ylimääräinen kehys. Toistoviiveen siirtäminen 60 ms taaksepäin tapahtuu puolestaan siten, että RTP-vastaanotossa kokonainen puhekehys hävitetään.

Kuviossa 1 RTP-siirto tapahtuu siis yhdyskäytävän GW ja päätelaitteen TE välillä pakettiverkon PDN yli. Yhdyskäytävän GW tehtävä on muuntaa keskukselta DXT PCM-linjaa pitkin tuleva piirikytketty puhe (tai muu data) IP-puhepaketeiksi ja päinvastoin. TETRA-infrastruktuurissa siirretään puhedataa kehyksissä, joten luonnollinen RTP-paketti sisältäisi yhden kehyksen puhedataa. Tällöin yhdessä RTP-paketissa olisi 60 ms puhetta, ja se vastaisi suoraan yhden puhekehyksen sisältöä. Toinen mahdollisuus on käyttää RTP-pakettia, joka sisältää vain puolikehyksen puhedataa (30 ms). Puolikehyspaketilla on seuraavat ominaisuudet verrattuna kokonaiskehyspakettiin: 1) Yhdyskäytävän vastaanottaessa puolikehyspaketteja sen täytyy odottaa, että kaksi pakettia on saapunut ennen ISI-kehyksen lähetyksen alkua. Molempia puhelohkoja koskevat ohjausbitit (BFI, C- tai U-varkaus) ovat nimittäin kehyksen alussa ja yhdyskäytävän täytyy määritellä ne puolikehyspakettien tyypin perusteella. 2) RTP-paketin kadotessa vain 30 ms puhetta puuttuu verrattuna 60 ms:in. Äänen laatua optimoitaessa on paketin pituus kompromissi kahden hahmottamisnäkökohdan välillä. Toinen ääripää on lyhyt paketti, jonka seurauksena puuttuvien pakettien määrä kasvaa kääntäen verrannollisesti pakettien kokoon, ja vääristymät tapahtuvat näin useammin. Toinen ääripää on pitkä paketti, jolloin vääristymät tapahtuvat harvemmin mutta jolla todennäköisyys kokonaisen foneemin häviämisestä ja näin ollen puheen ymmärrettävyyden huononemisesta kasvaa varsinkin kun paketin pituus on yli 20 ms. Jälkimmäinen raja on nimittäin lyhyin foneemin pituus. 3) Kaistanleveyden kannalta pitkä paketti on kuitenkin tehokkaampi, sillä otsikoiden (Ethernet + IP + UDP + RTP) pituus (36-40 tavua) on hyötykuorman pituuteen verrattuna (18 tavua/puhelohko tai 36 tavua/puhekehys) jo pitkä. Otsikoiden osuutta paketissa voidaan pienentää käyttämällä kahta tekniikkaa. Multipleksauksen avulla

voidaan useita puhekanavia pakata samaan RTP-pakettiin ja näin pienentää otsikoiden osuutta. Tämä on varsin kiinnostavaa keskuksesta-käyttöpaikkaan-yhteyttä varten, sillä kaikki ryhmäpuhelut ja yksilöpuhelu voidaan näin lähettää samassa paketissa. Toinen tekniikka, joka soveltuu sarjayhteyksiin, on otsikoiden kompressio. Sen avulla voidaan IP/UDP/RTP-otsikkoa pienentää huomattavasti (2-4 tavuihin) ja näin säästää kaistanleveyttä. Paremman äänenlaadun saavuttamiseksi on lyhyt RTP-paketti (30 ms) näin ollen edullisempi.

Puhelohkoja voidaan varastaa kehyksen sisältä joko verkon (C-varastettu) tai käyttäjän (U-varastettu) tarkoitukseen. Esimerkiksi päästäpäähän -salausta käytettäessä päätelaitteet varastavat yhden puhelohkon omaan tarkoitukseensa 1 - 4 kertaa sekunnissa tahdistusvektorin välittämiseen kuten edellä on selitetty.

ACELP-koodekkeja tuetaan RTP-standardissa ja monessa IP-puhepäätelaitteessa, mutta TETRA-kohtaista ACELP:iä ei RTP-standardi tue. Puheen siirtämistä varten voidaan käyttää RTP-pakettia, jossa on esimerkiksi seuraavat asetukset: RTP-versio 2, ei täytettä, ei laajennusta, ei CRSC lähteitä, ei merkitsintä, kuorman tyyppi: 8 (sama kuin A-laki), aikaleima kasvaa 240 yksiköllä jokaista pakettia kohti. Tämä vastaa TETRA:n 8000 Hz näytteenottokelloa ja 30 ms näytteenpituutta. Hyötykuormassa esiintyvät seuraavat tiedot: kolme ensimmäistä bittiä ilmaisevat, onko kehysvirhebitti (BFI) asetettu, onko hyötykuormassa ääni vai data, ja onko mahdollisesti kyseessä C- tai U-varastettu puhelohko; muut ensimmäisen tavun bitit eivät ole käytössä; seuraavat 137 bittiä ovat varsinaista dataa, ja ne vastaavat yhtä puhelohkoa. Hyötykuorman loput bitit ovat 0.

Edellä kuvattu yhdyskäytävän GW toiminta piirikytketyn ja pakettikytketyn yhteyden välillä on vain eräs mahdollinen toteutustapa ja yhdyskäytävän GW toiminta voi poiketa tästä ilman, että sillä on merkitystä keksinnön perusajatuksen kannalta.

Kuviossa 1 esitetty päätelaite TE voi olla puhepäätelaite tai datapäätelaite ja keksintöä voidaan soveltaa esimerkiksi ääniyhteyksiin, kuvayhteyksiin tai datayhteyksiin, jotka vaativat reaaliaikaista tiedonsiirtoa. Päätelaite TE voi olla esimerkiksi matkaviestin, käyttöpaikan työasema, tukiasema tai jokin muu verkkoelementti. Päätelaite TE ei ole välttämättä suoraan kytketty pakettiverkkoon PDN vaan päätelaitteen TE ja pakettiverkon PDN välillä voi olla esimerkiksi toinen TETRA-verkko. Tällöin myös pakettiyhteyden PDN toisessa päässä on yhdyskäytäväelementti. Välissä voi olla myöskin jokin muu yhteys

tai useampia pakettiyhteyksiä. Jos päätelaite TE on kuvion 1 mukaisesti kytketty suoraan pakettiverkkoon PDN, toimii se RTP-siirron toisena osapuolena olennaisesti samalla tavoin, kuin jo edellä on kuvattu yhdyskäytävän GW osalta.

Keksinnön mukaisesti suoritetaan pakettiyhteyden PDN vastaanottavassa päässä GW tai TE toistoviiveen muutos tiedon lähetyksen, esimerkiksi puheenvuoron tai puhelun, aikana, sellaisena ajankohtana, että muutoksen jälkeen seuraavaksi siirrettävä kehys käsittää tahdistusvektorin. Edullisen suoritusmuodon mukaisesti tämä tapahtuu siten, että tarkkaillaan pakettiyhteyden PDN vastaanottavassa päässä GW tai TE saapuvia kehyksiä ja tunnistetaan kehyksissä olevat tahdistusvektorit. Tällöin voidaan mahdollisesti tarvittava toistoviiveen muutos ajoittaa sellaiseen ajankohtaan, että seuraavaksi edelleen lähetettävä kehys käsittää tahdistusvektorin. Esimerkkinä voidaan tarkastella tilannetta, jossa kuviossa 1 matkaviestimen MS ja päätelaitteen TE välillä on puhelu, joka kulkee pakettiyhteyden PDN kautta RTP-protokollan mukaisesti. RTP-protokollan mukainen tiedonsiirto tapahtuu tällöin protokollaa tukevien yhdyskäytävän GW ja päätelaitteen TE välillä. Tällöin yhdyskäytävä GW, joka on pakettiyhteyden PDN vastaanottava pää päätelaitteelta TE tulevan liikenteen suhteen, tarkkailee päätelaitteelta TE saapuvia kehyksiä vastaanottopuskurissaan ja tunnistaa niissä olevat tahdistusvektorit. Kun RTP-algoritmin mukaisesti havaitaan tarve muuttaa toistoviivettä, suoritetaan muutos yhdyskäytävässä GW sellaisella hetkellä, että muutoksen jälkeen seuraavaksi yhdyskäytävästä GW matkaviestimen MS suuntaan edelleensiirrettävä kehys käsittää tahdistusvektorin. Tällöin matkaviestimen MS salausalgoritmi tahdistuu välittömästi muutoksen jälkeen, vaikka kehysjonosta olisi poistettu kehyksiä tai siihen olisi lisätty kehyksiä, koska tyhjää kohtaa tai ylimääräisiä kehyksiä seuraava kehys käsittää tahdistusvektorin. Vastaavalla tavalla päätelaite TE, joka on pakettiyhteyden PDN vastaanottava pää matkaviestimeltä MS tulevan liikenteen suhteen, tarkkailee yhdyskäytävältä GW saapuvia kehyksiä ja tunnistaa niissä olevat tahdistusvektorit. Kun RTP-algoritmin mukaisesti havaitaan tarve muuttaa toistoviivettä, suoritetaan muutos päätelaitteessa TE sellaisella hetkellä, että muutoksen jälkeen seuraavaksi salauksen purkuun ja toistettavaksi edelleensiirrettävä kehys käsittää tahdistusvektorin, jolloin päätelaitteen TE salauksen purku tahdistuu välittömästi muutoksen jälkeen. Toistoviiveen ohjaus päätelaitteessa TE tapahtuu siis kuvion 2 kaavioon viitaten ennen suodatinlohkoa 25. Kuviossa 7A on havainnollistettu keksinnön

mukaista toistoviiveen pienentämistä pakettiyhteyden PDN vastaanottavassa päässä GW tai TE. Kuviossa on esitetty vastaanotettava kehysjono 73, josta poistetaan yksi tai useampia kehyksiä 71 ja edelleentoimitusta varten saadaan kehysjono 74. Keksinnön mukaisesti kehysten 71 poisto tapahtuu juuri ennen tahdistusvektorin sisältävää kehystä SVF. Vastaavalla tavalla Kuviossa 7B on havainnollistettu keksinnön mukaista toistoviiveen kasvattamista pakettiyhteyden PDN vastaanottavassa päässä GW tai TE. Kuviossa on esitetty vastaanotettava kehysjono 75, johon lisätään yksi tai useampia kehyksiä 72 ja edelleentoimitusta varten saadaan kehysjono 76. Keksinnön mukaisesti kehysten 72 lisäys tapahtuu juuri ennen tahdistusvektorin sisältävää kehystä SVF.

Alan ammattilaiselle on ilmeistä, että tekniikan kehittyessä keksinnön perusajatus voidaan toteuttaa monin eri tavoin. Keksintö ja sen suoritusmuodot eivät siten rajoitu yllä kuvattuihin esimerkkeihin vaan ne voivat vaihdella patenttivaatimusten puitteissa.

Patenttivaatimukset

1. Menetelmä päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta, joka tahdistetaan lähettämällä ajoittain tahdistusvektoreita mainituissa kehyksissä, ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä, jolloin siirrettävän tiedon toistoviivettä voidaan kasvattaa lisäämällä yksi tai useampia ylimääräisiä kehyksiä siirrettävään kehysjonoon ja pienentää poistamalla yksi tai useampia kehyksiä siirrettävästä kehysjonosta, t u n n e t t u siitä, että

suoritetaan tiedon lähetyksen aikana tapahtuva toistoviiveen muuttaminen sellaisella hetkellä, että muutoksen jälkeen seuraavaksi siirrettävä kehys käsittää tahdistusvektorin.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että

tarkkaillaan pakettikytketyn yhteyden vastaanottavassa päässä saapuvia kehyksiä,

tunnistetaan kehyksissä olevat tahdistusvektorit ja

suoritetaan pakettikytketyn yhteyden vastaanottavassa päässä toistoviiveen muuttaminen sellaisella hetkellä, että muutoksen jälkeen pakettikytketyn yhteyden vastaanottavassa päässä seuraavaksi edelleensiirrettävä kehys käsittää tahdistusvektorin.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että pakettikytketty yhteys käyttää Internet-protokollaa.

4. Patenttivaatimuksen 1, 2 tai 3 mukainen menetelmä, t u n n e t t u siitä, että tietoliikenneyhteys kuuluu TETRA-järjestelmään.

5. Jonkin patenttivaatimuksista 1-4 mukainen menetelmä, t u n n e t t u siitä, että salaus suoritetaan avainsarjan avulla, jonka luomisessa käytetään alustusvektoria.

6. Jonkin patenttivaatimuksista 1–5 mukainen menetelmä, t u n n e t t u siitä, että tahdistusvektori käsittää alustusvektorin.

7. Järjestely päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta, joka tahdistetaan lähettämällä ajoittain tahdistusvektoreita mainituissa kehyksissä, ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä (PDN), jolloin siirrettävän tiedon toistoviivettä voidaan kasvattaa lisäämällä yksi tai useampia

ylimääräisiä kehyksiä siirrettävään kehysjonoon ja pienentää poistamalla yksi tai useampia kehyksiä siirrettävästä kehysjonosta, t u n n e t t u siitä, että

järjestely käsittää toistoviiveen säätövälineet (GW, TE), jotka on sovitettu suorittamaan tiedon lähetyksen aikana tapahtuva toistoviiveen muuttaminen sellaisella hetkellä, että muutoksen jälkeen seuraavaksi siirrettävä kehys käsittää tahdistusvektorin.

8. Patenttivaatimuksen 7 mukainen järjestely, t u n n e t t u siitä, että toistoviiveen säätövälineet on lisäksi sovitettu

tarkkailemaan pakettikytketyn yhteyden (PDN) vastaanottavassa päässä saapuvia kehyksiä,

tunnistamaan kehyksissä olevat tahdistusvektorit ja

suorittamaan pakettikytketyn yhteyden (PDN) vastaanottavassa päässä toistoviiveen muuttaminen sellaisella hetkellä, että muutoksen jälkeen pakettikytketyn yhteyden vastaanottavassa päässä seuraavaksi edelleensiirrettävä kehys käsittää tahdistusvektorin.

9. Patenttivaatimuksen 7 tai 8 mukainen järjestely, t u n n e t t u siitä, että pakettikytketty yhteys käyttää Internet-protokollaa.

10. Patenttivaatimuksen 7, 8 tai 9 mukainen järjestely, t u n n e t t u siitä, että tietoliikenneyhteys kuuluu TETRA-järjestelmään.

11. Jonkin patenttivaatimuksista 7–10 mukainen järjestely, t u n n e t t u siitä, että salaus suoritetaan avainsarjan avulla, jonka luomisessa käytetään alustusvektoria.

12. Jonkin patenttivaatimuksista 7–11 mukainen järjestely, t u n n e t t u siitä, että tahdistusvektori käsittää alustusvektorin.

13. Verkkoelementti päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta, joka tahdistetaan lähettämällä ajoittain tahdistusvektoreita mainituissa kehyksissä, ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä (PDN), joka käsittää verkkoelementin (GW, TE), joka voi kasvattaa siirrettävän tiedon toistoviivettä lisäämällä yhden tai useampia ylimääräisiä kehyksiä siirrettävään kehysjonoon ja pienentää siirrettävän tiedon toistoviivettä poistamalla yhden tai useampia kehyksiä siirrettävästä kehysjonosta, t u n n e t t u siitä, että

verkkoelementti on sovitettu suorittamaan tiedon lähetyksen aikana tapahtuva toistoviiveen muuttaminen sellaisella hetkellä, että muutoksen jälkeen seuraavaksi siirrettävä kehys käsittää tahdistusvektorin.

14. Patenttivaatimuksen 13 mukainen verkkoelementti, t u n n e t t u siitä, että verkkoelementti on lisäksi sovitettu

tarkkailemaan pakettikytketyn yhteyden (PDN) vastaanottavassa päässä saapuvia kehyksiä,

tunnistamaan kehyksissä olevat tahdistusvektorit ja

suorittamaan pakettikytketyn yhteyden (PDN) vastaanottavassa päässä toistoviiveen muuttaminen sellaisella hetkellä, että muutoksen jälkeen pakettikytketyn yhteyden vastaanottavassa päässä seuraavaksi edelleensiirrettävä kehys käsittää tahdistusvektorin.

15. Patenttivaatimuksen 13 tai 14 mukainen verkkoelementti, t u n n e t t u siitä, että pakettikytketty yhteys käyttää Internet-protokollaa.

16. Patenttivaatimuksen 13, 14 tai 15 mukainen verkkoelementti, t u n n e t t u siitä, että tietoliikenneyhteys kuuluu TETRA-järjestelmään.

17. Jonkin patenttivaatimuksista 13–16 mukainen verkkoelementti, t u n n e t t u siitä, että salaus suoritetaan avainsarjan avulla, jonka luomisessa käytetään alustusvektoria.

18. Jonkin patenttivaatimuksista 13–17 mukainen verkkoelementti, t u n n e t t u siitä, että tahdistusvektori käsittää alustusvektorin.

19. Jonkin patenttivaatimuksista 13–18 mukainen verkkoelementti, t u n n e t t u siitä, että verkkoelementti on TETRA käyttöpaikan työasema.

20. Jonkin patenttivaatimuksista 13–18 mukainen verkkoelementti, t u n n e t t u siitä, että verkkoelementti on tukiasema.

21. Jonkin patenttivaatimuksista 13–18 mukainen verkkoelementti, t u n n e t t u siitä, että verkkoelementti on mediayhdyskäytävä.

(57) Tiivistelmä

Menetelmä ja järjestely päästä-päähän -tahdistuksen ylläpitämiseksi tietoliikenneyhteydellä, jolla siirretään tietoa kehyksissä olennaisesti reaaliaikaisesti ja käyttäen tahdistettua päästä-päähän -salausta, joka tahdistetaan lähettämällä ajoittain tahdistusvektoreita mainituissa kehyksissä, ja jolloin ainakin osa tietoliikenneyhteydestä muodostuu pakettikytketystä yhteydestä (PDN), jolloin siirrettävän tiedon toistoviivettä voidaan kasvattaa lisäämällä yksi tai useampia ylimääräisiä kehyksiä siirrettävään kehysjonoon ja pienentää poistamalla yksi tai useampia kehyksiä siirrettävästä kehysjonosta, jolloin järjestely käsittää toistoviiveen säätövälineet (GW, TE), jotka on sovitettu suorittamaan tiedon lähetyksen aikana tapahtuva toistoviiveen muuttaminen sellaisella hetkellä, että muutoksen jälkeen seuraavaksi siirrettävä kehys käsittää tahdistusvektorin.
(Kuvio 1)

Fig. 1

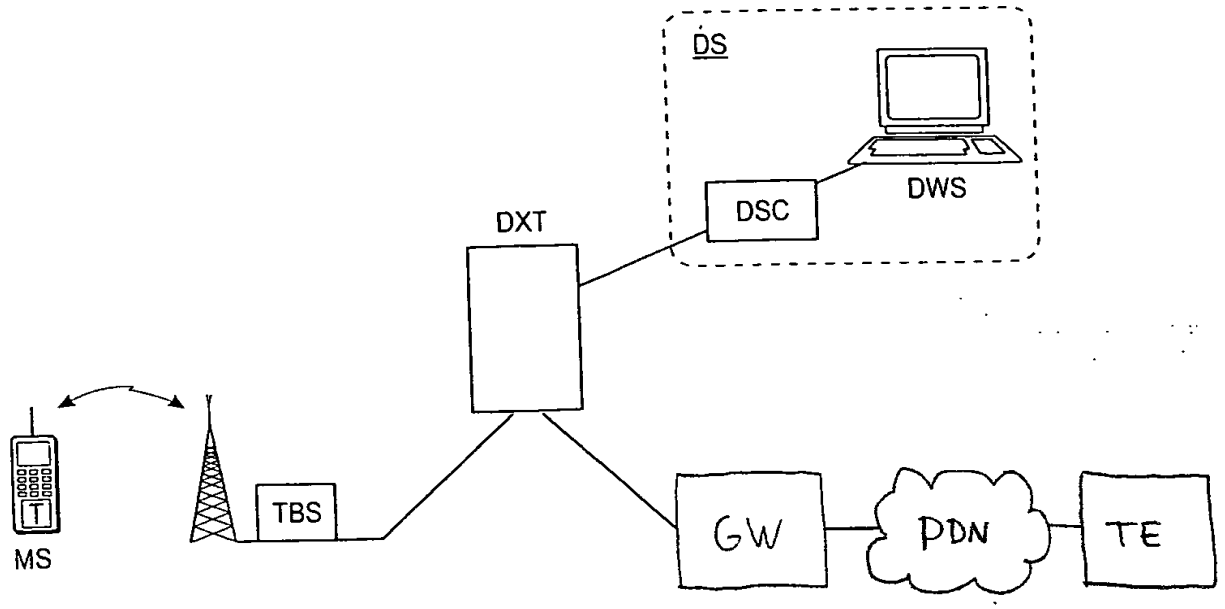
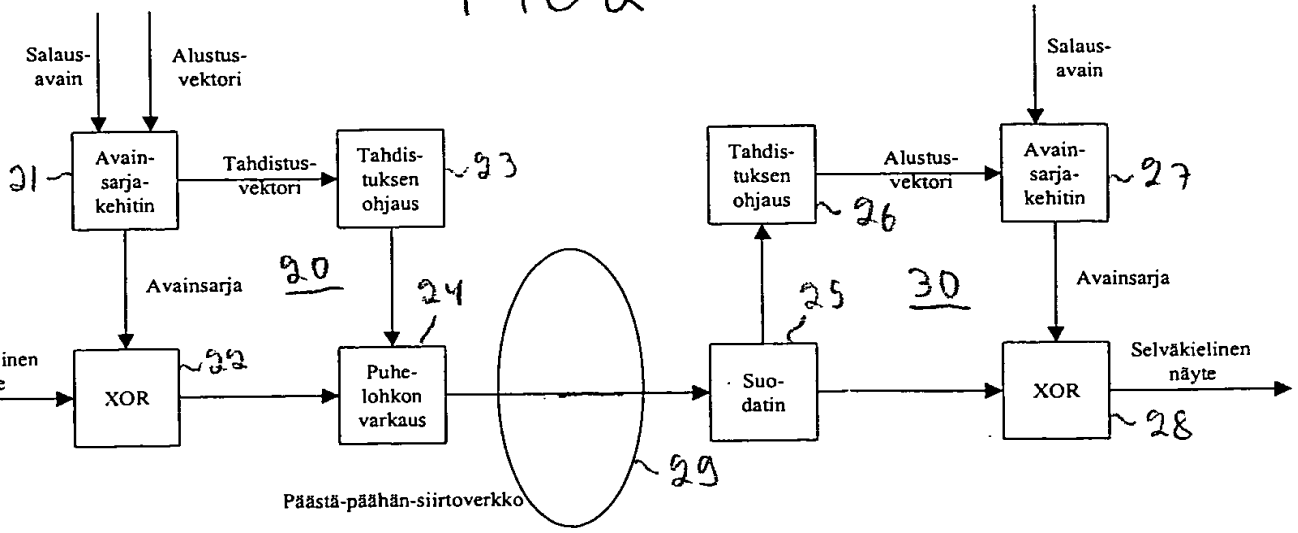

DS
DWS
DSC
DXT
MS
TBS
GW
PDN
TE

FIG2


Salaus-avain
Alustus-vektori
Avain-sarja-kehitin
21
Tahdistus-vektori
Tahdis-tuksen ohjaus
23
Avainsarja
20
24
Selväkielinen näyte
XOR
22
Puhe-lohkon varkaus
Päästä-päähän-siirtoverkko
29
Tahdis-tuksen ohjaus
26
Alustus-vektori
Salaus-avain
Avain-sarja-kehitin
27
25
30
Avainsarja
Suo-datin
XOR
Selväkielinen näyte
28

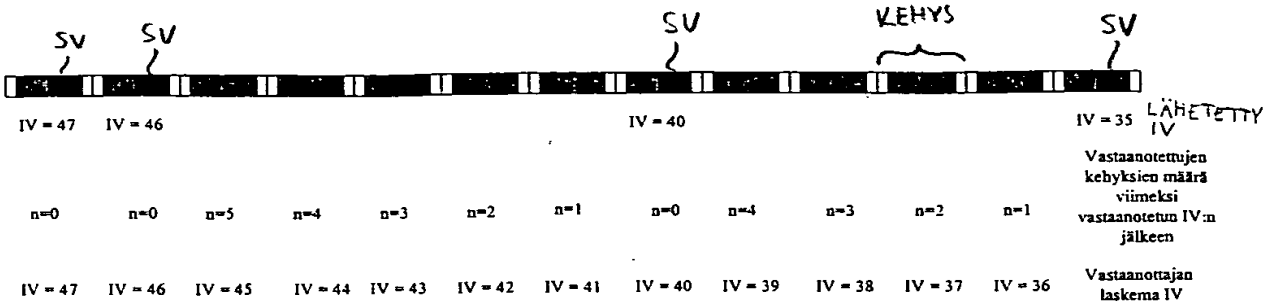

SV
SV
SV
KEHYS
SV
IV = 47
IV = 46
IV = 40
IV = 35
LÄHETETTY IV
Vastaanotettujen kehyksien määrä viimeksi vastaanotetun IV:n jälkeen
n=0
n=0
n=5
n=4
n=3
n=2
n=1
n=0
n=4
n=3
n=2
n=1
Vastaanottajan laskema IV
IV = 47
IV = 46
IV = 45
IV = 44
IV = 43
IV = 42
IV = 41
IV = 40
IV = 39
IV = 38
IV = 37
IV = 36

FIG3

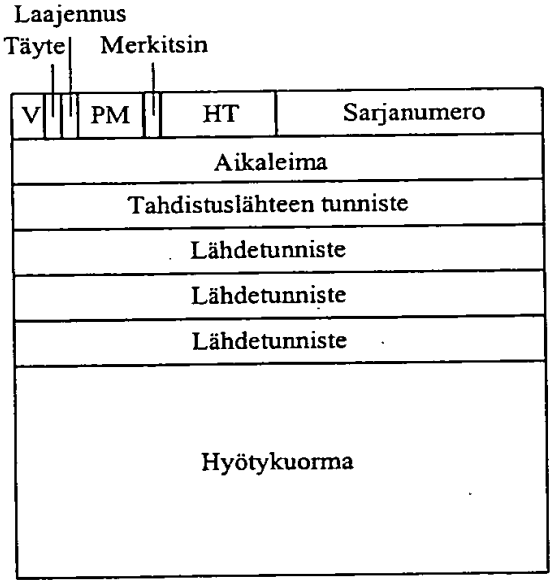

Laajennus
Täyte
Merkitsin
V
PM
HT
Sarjanumero
Aikaleima
Tahdistuslähteen tunniste
Lähdetunniste
Lähdetunniste
Lähdetunniste
Hyötykuorma

FIG4

FIG 5

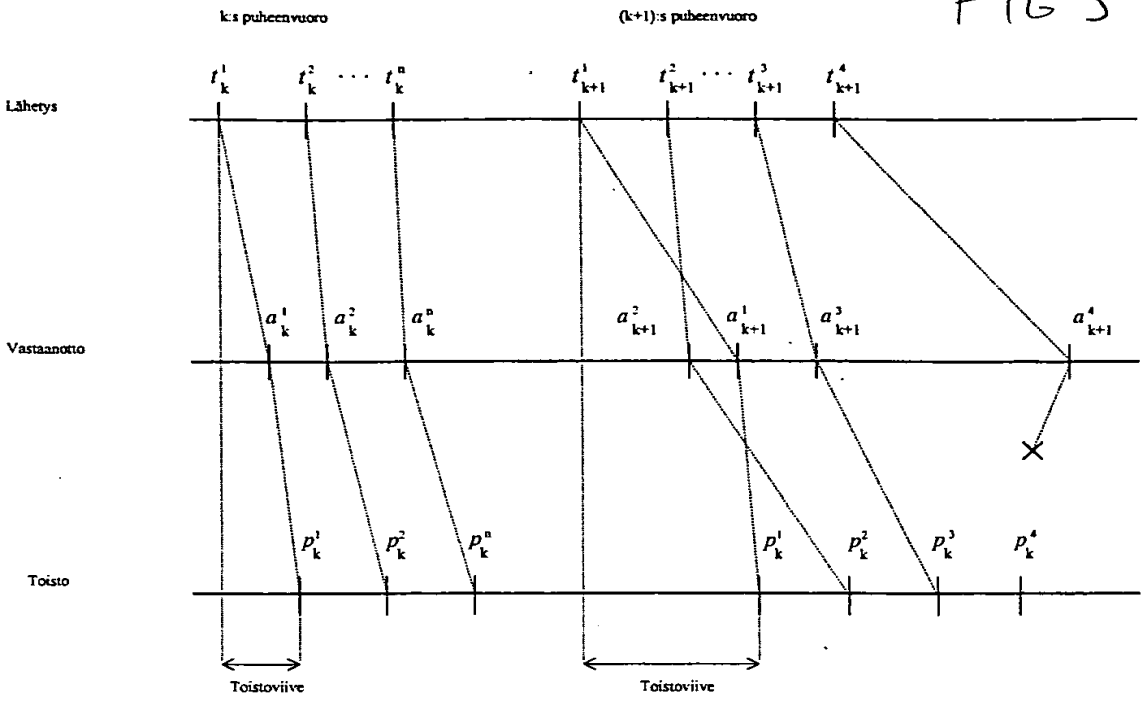
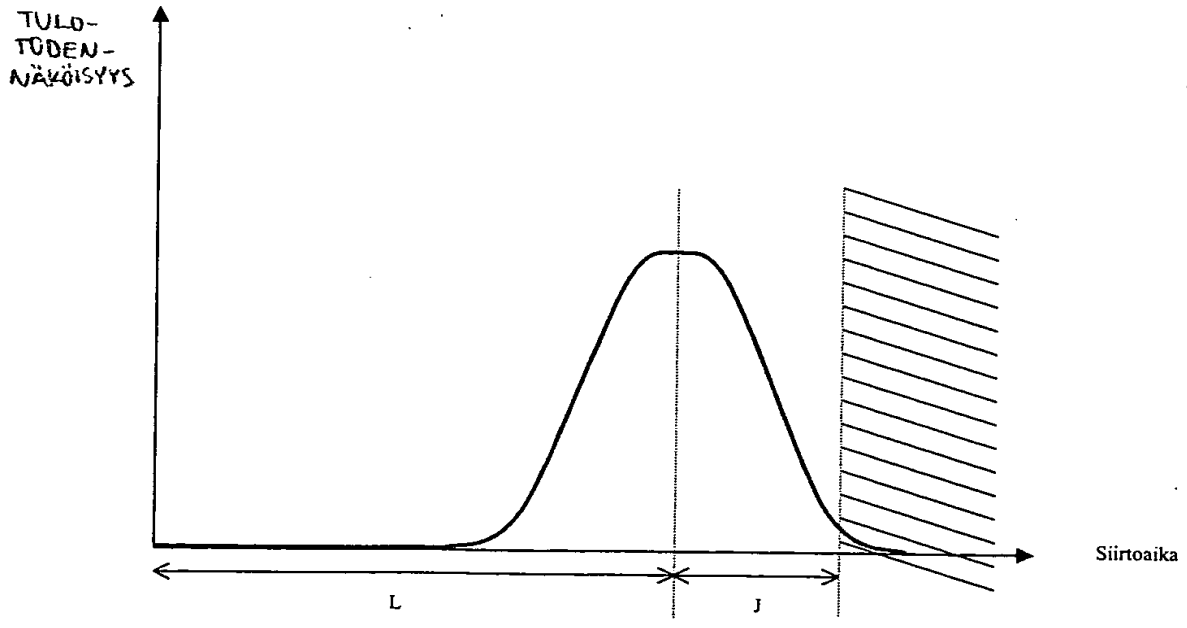

k:s puheenvuoro
(k+1):s puheenvuoro
Lähetys
Vastaanotto
Toisto
Toistoviive
Toistoviive

FIG 6


TULO-
TODEN-
NÄKÖISYYS
Siirtoaika
L
J

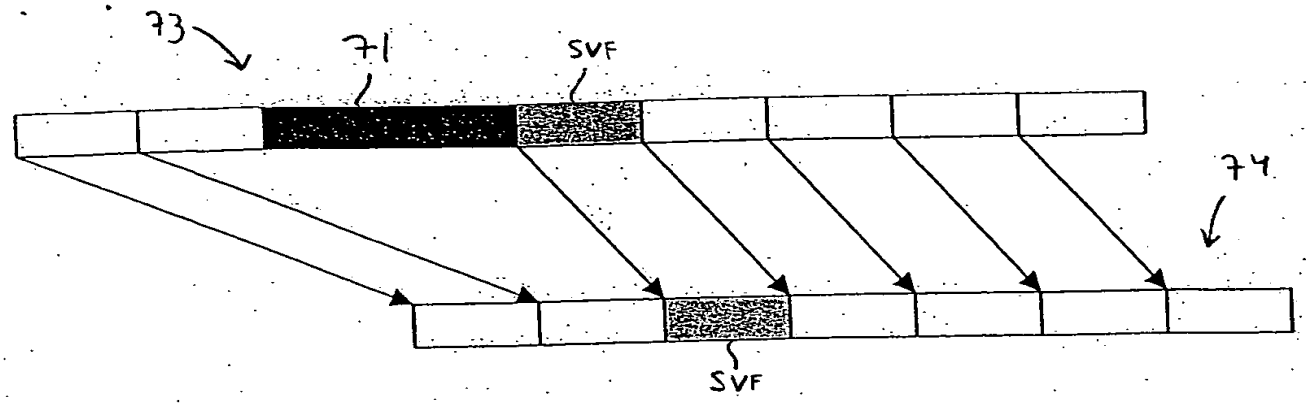


FIG7A

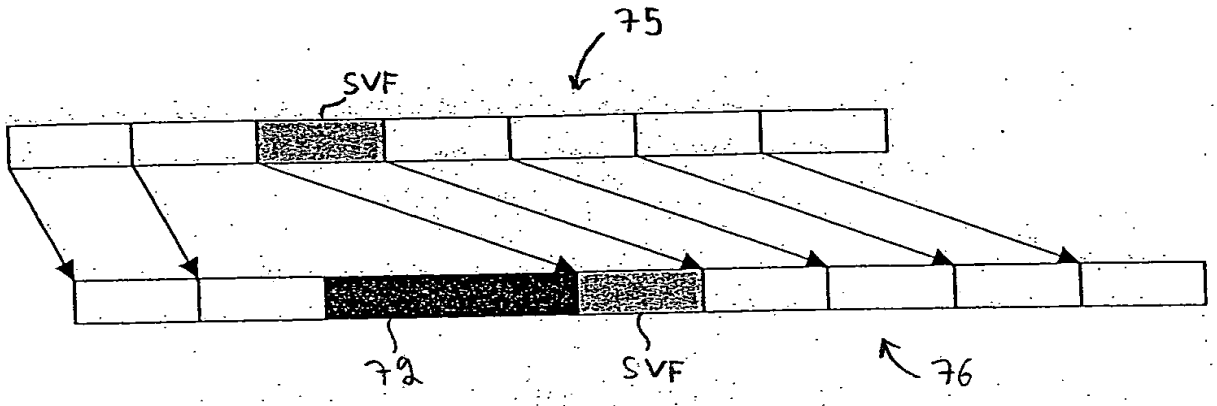


FIG7B